

VIRTUALISATION : MODULE-1

MAJEURE INFRASTRUCTURE 2020

Présentation du cours

2

- ▣ Présentation de VMware vSphere 6.7
- ▣ Installation et configuration d'un serveur ESXi
- ▣ Installation et configuration d'un vCenter
- ▣ vSphere et le réseau
- ▣ vSphere et le stockage
- ▣ Création et gestion de machines virtuelles
- ▣ Migration et import de machines virtuelles
- ▣ Gestion des logs

Installation et configuration d'un ESXi

3

- vSphere 6.7 contient 2 composants :
 - ▣ VMware ESXi Server
 - Hyperviseur, peut fonctionner de manière autonome
 - ▣ VMware vCenter
 - Pilotage des hyperviseurs ESXi

Présentation de vSphere 6

4

□ Configuration des machines virtuelles :

	vSphere 5.0 🔗	vSphere 5.1 🔗	vSphere 5.5 🔗	vSphere 6.0 🔗	vSphere 6.5 🔗	vSphere 6.7 🔗
Virtual CPU	32	64	64	128	128	128
Virtual RAM	1 TB	1 TB	1 TB	4 TB	6128 GB	6128 GB
Max VMDK size	2 TB – 512 B	2 TB – 512 B	62 TB	62 TB	62 TB	62 TB
Virtual SCSI adapters	4	4	4	4	4	4
Virtual SCSI targets per adapter	15	15	15	15	15	64
Virtual SCSI targets	60	60	60	60	60	256
Virtual NVMe adapters	NA	NA	NA	NA	4	4
Virtual NVMe targets per adapter	NA	NA	NA	NA	15	15
Virtual NVMe targets	NA	NA	NA	Na	60	60
Virtual NICs	10	10	10	10	10	10

Présentation de vSphere 6

5

□ Configuration des ESXi :

	vSphere 5.0 🔗	vSphere 5.1 🔗	vSphere 5.5 🔗	vSphere 6.0 🔗	vSphere 6.5 🔗	vSphere 6.7 🔗
Logical CPU	160	160	320	480	576	768
Physical RAM	2 TB	2 TB	4 TB	12 TB	12 TB	16 TB
NUMA Nodes	8 nodes	8 nodes	16 nodes	16 nodes	16	16
Virtual CPU	2048	2048	4096	4096	4096	4096
Volumes	256	256	256	256	512	1024
Virtual disks	2048	2048	2048	2048	2048	2048
Virtual Machines	512	512	512	1024	1024	1024

vSphere

6

- Version la plus récente : 6.7 (2018)
- Plusieurs niveau de licences (essential, standard, enterprise plus, enterprise plus + operations, ROBO, ...)
- Voir : <http://www.vmware.com/products/vsphere.html>

Installation et configuration d'un ESXi

7

- Avant l'installation, vérifier que votre matériel est dans la HCL :
 - ▣ Serveurs
 - ▣ Stockage
 - ▣ Cartes d'extension

Installation et configuration d'un ESXi

8

- Méthodes d'installation :
 - ▣ Manuelle
 - DVD/USB
 - ▣ Silencieuse/Automatique
 - HTTP, NFS, FTP, DVD, Autodeploy
- On peut installer le serveur sur les disques locaux ou sur une clé USB/carte flash

Installation et configuration d'un ESXi

9

TP

Installation d'un serveur ESXi

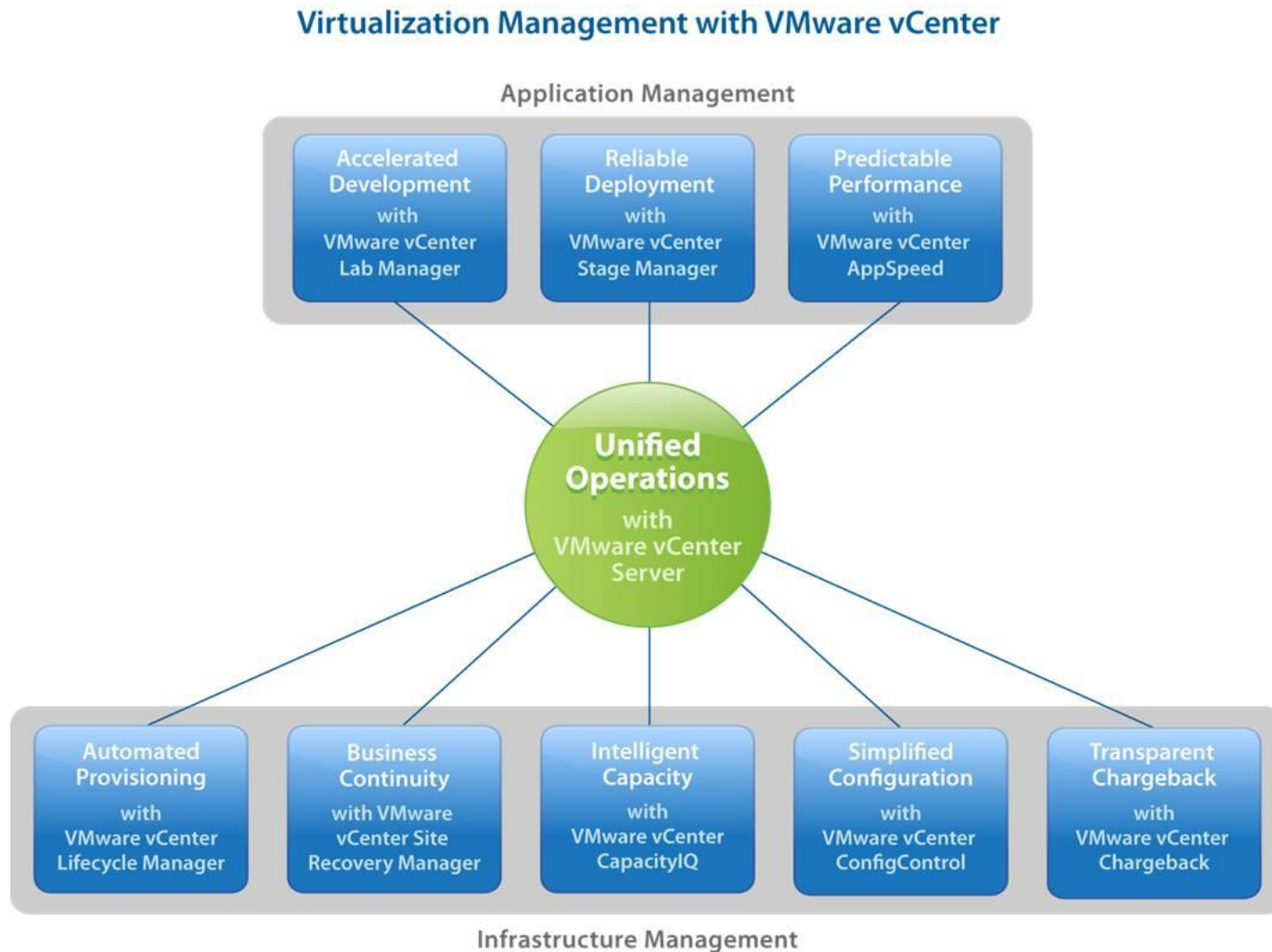
Installation et configuration d'un vCenter

10

- Le vCenter est le point central de la gestion d'une infrastructure vSphere

- Fonctionnalités:
 - ▣ Gestion des ressources
 - ▣ Template
 - ▣ Déploiement et gestion des VMs
 - ▣ Tâches planifiées
 - ▣ Statistiques
 - ▣ Alarmes
 - ▣ Management des hyperviseurs

Installation et configuration d'un vCenter



Disponibilité du vCenter

- Solutions de haute disponibilité pour le vCenter :
 - ▣ HA vSphere (si c'est une VM)
 - ▣ Standby server
 - ▣ HA appliance (à partir de 6.5)

Types de vCenter

- Installation manuelle des composants sur un OS Windows server (ne sera plus supporté en vSphere 7)
 - ▣ BDD : Windows SQL, Oracle

- Virtual appliance (vApp) fournie par VMware (architecture de référence en 6.7)
 - ▣ OS : Linux (Photon de VMware)
 - ▣ BDD : PostgreSQL

Installation et configuration d'un vCenter

14

TP

Installation d'un serveur vCenter

vSphere et le réseau

15

- Définissez l'architecture dont vous avez besoin :
 - ▣ Type de trafic à véhiculer
 - ▣ Débit des liens réseaux
 - ▣ Besoins d'isolation
 - ▣ Nombre de cartes réseaux et ports de switches disponibles
 - ▣ ..

vSphere et le réseau

16

- vSwitch ≠ switchs physiques
 - ▣ Gestion différente des MAC
 - ▣ Pas de STP
 - ▣ Pas de négociation dynamique pour le **D**ynamic **T**runking **P**rotocol et **P**ort **A**ggregation **P**rotocol

- Quelques définitions :
 - ▣ Port/Port group :
 - ▣ Vmkernel port : port réseau virtuel délivrant des services pour l'hyperviseur
 - ▣ Virtual machine port group : groupe de ports qui partagent une configuration commune
 - ▣ Acces port : port réseau qui ne transport qu'un vlan

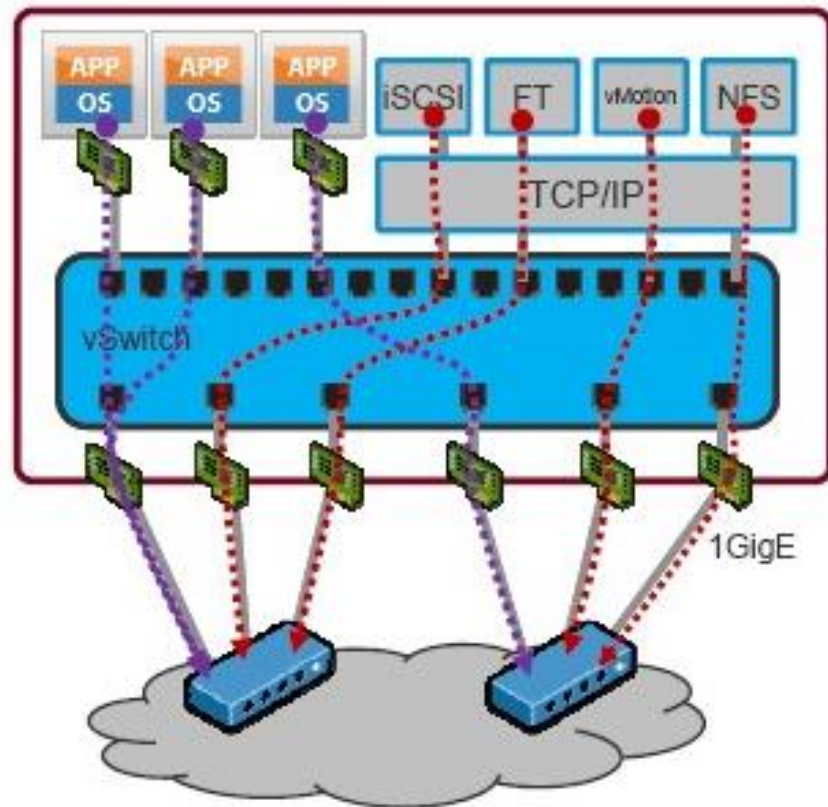
Standard vSwitch

17

- Standard vSwitch
 - ▣ Communication entre les VMs d'un même hyperviseur
 - ▣ Communication entre les VMs d'hyperviseurs différents
 - ▣ Communication entre les VMs et les autres machines du réseau
 - ▣ Communication entre les Vmkernel et le reste du réseau
 - ▣ Les vSwitch sont propres à chaque ESXi

Standard vSwitch

18



Standard vSwitch

19

- Les switches virtuels doivent être reliés à des cartes réseaux physiques (uplink) pour communiquer avec l'extérieur

- Techniques de répartition du trafic des VM:
 - Source MAC Load Balancing
 - Originating virtual port ID
 - IP Hash

Standard vSwitch

20

- Trois possibilités pour gérer les Vlan :
 - ▣ Arrêt du tag au niveau du Switch (**E**xternal **S**witch **T**agging)
 - ▣ Arrêt du tag au niveau du vSwitch (**V**irtual **S**witch **T**agging)
 - ▣ Arrêt du tag dans la VM (**V**irtula **G**uest **T**agging)

- Traffic Shaping:
 - ▣ Permet de limiter le trafic sortant des VM
 - ▣ Trois paramètres :
 - Average Bandwith (Kbits/s)
 - Peak Bandwith (Kbits/s)
 - Burst size (Kbyte)

Limites des Standard vSwitch en v5

21

Élément	Limite
Nombre de vSwitch	248
Ports par vSwitch	4088
Ports par hôtes	4096
Port groups par vSwitch	512
Port groups par hôtes	512
Uplinks par vSwitch	32
Vmkernel nics	16
Virtual NICs par hôte	4096

Standard vSwitch

22

TP

Configuration de vSwitch

Distributed vSwitch

23

- Mêmes fonctionnalités de base que les vSwitchs...
- Avec en plus :
 - ▣ CDP/LLDP
 - ▣ Gestion de la sécurité par port
 - ▣ Statistiques avancées
 - ▣ Traffic shaping par port
 - ▣ Private vlan
 - ▣ Network I/O control
 - ▣ LACP (à partir de 5.5)
 - ▣ NetFlow

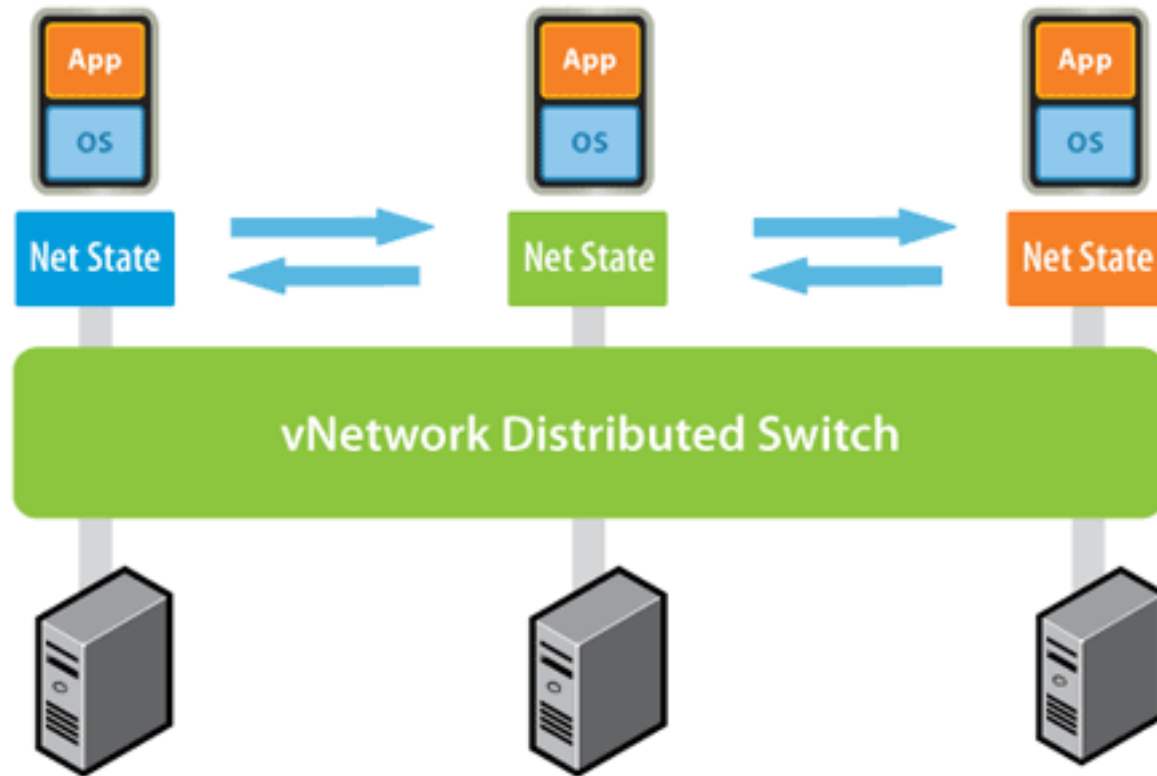
Distributed vSwitch

24

- Les dvSwitch sont bien plus puissants mais ... ne sont pas disponibles dans toutes les versions
- Ils ne se configurent pas sur chaque ESXi mais au niveau datacenter
- Le vCenter est chargé de distribuer leur configuration

Distributed vSwitch

25



Limites des Distributed vSwitch en v5

26

Elément	Limite
dvSwitch par vCenter	16
dvSwitch par hôte	16
dvPort group par dvSwitch	512
Nombre de ports par dvSwitch	8000
Nombre d'hôte par dvSwitch	300
VM par dvSwitch	3000
Vlans ou PVlans	512

Distributed vSwitch

27

TP

Configuration de dvSwitch

vSphere et le stockage

28

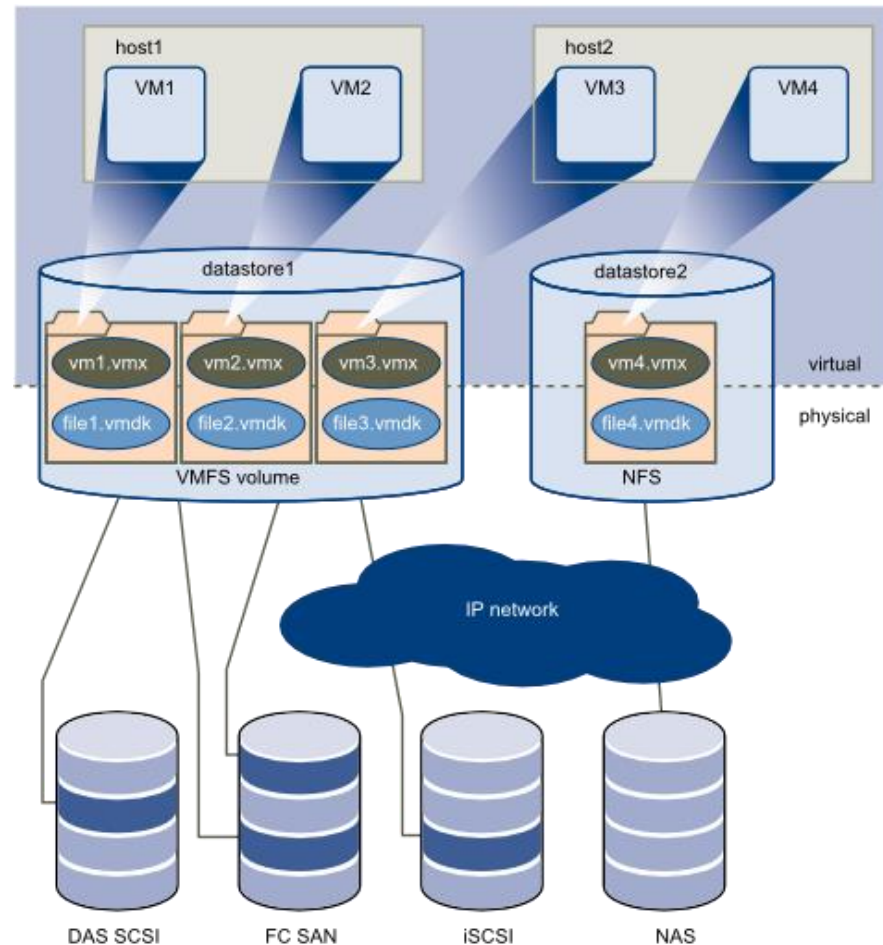
- 4 types de stockages utilisables :
 - ▣ Disques locaux (mécaniques, SSD, ..)
 - ▣ Partages NFS
 - ▣ iSCSI, FCoE
 - ▣ Fibre channel et FC-NVMe

Présentation du stockage aux VMs

29

- Via des disques durs virtuels hébergés dans des pools de stockage (Datastore, NAS)
- Directement à la VM
 - ▣ Physical Raw device mapping (pass-through)
 - Clusters Windows
 - ▣ Virtual Raw device mapping (Vmware)
- Dans la VM
 - ▣ iSCSI
 - ▣ NFS

Présentation du stockage aux VMs



Le thin provisioning

31

- Permet de faire de la sur allocation
- Plusieurs niveaux
 - ▣ Dans la VM (OS)
 - ▣ Sur le datastore (hyperviseur)
 - ▣ Sur les volumes (baie de stockage)
- Natif sur les NAS
- Problème de suivi des différents niveaux

VMFS

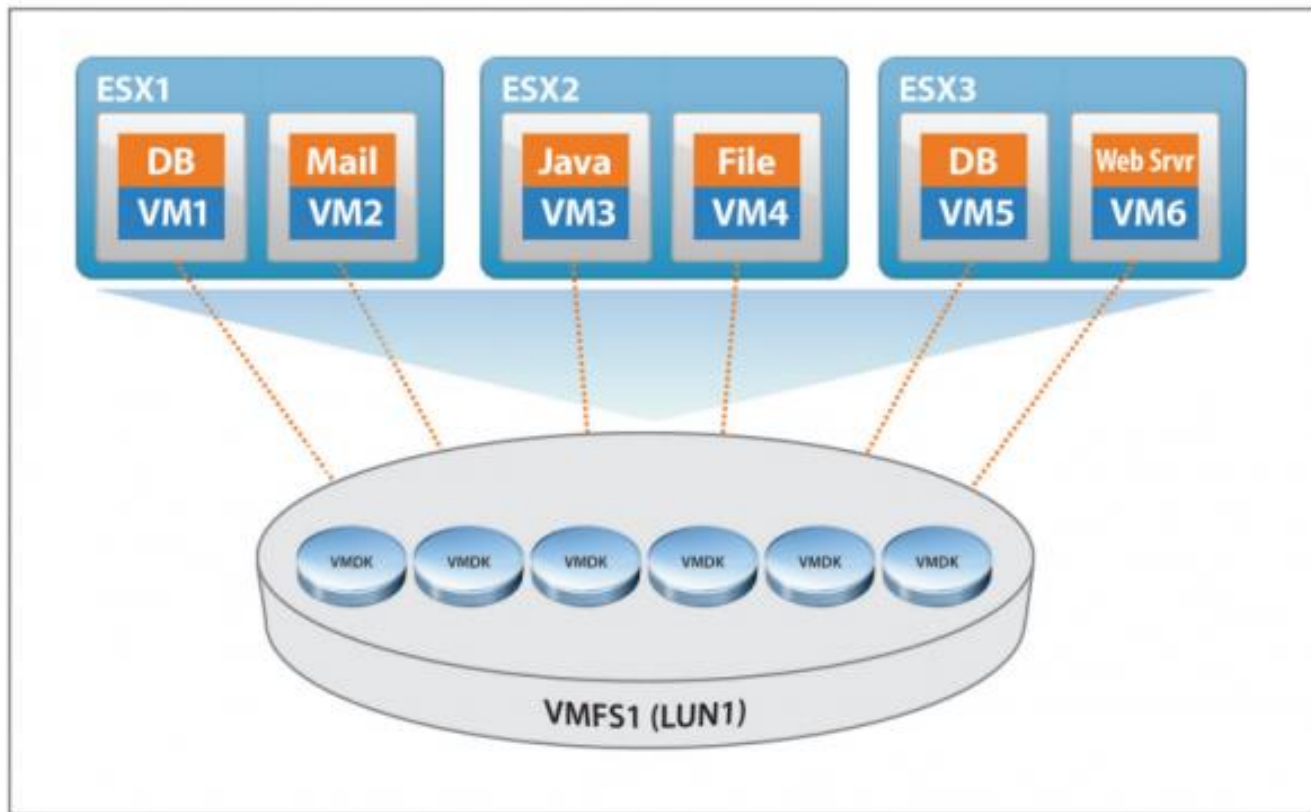
32

- C'est un système de fichier développé par VMware
 - ▣ Version 5 en vSphere 5, 6 en vSphere 6.5
 - ▣ FS de type cluster
 - ▣ Système de verrouillage simplifié
 - ▣ Peut être créé sur du stockage local ou distant
 - ▣ Taille max : 64TB-512 bytes

- On peut agrandir un VMFS :
 - ▣ En ajoutant un lun/disque (on utilise un « extend »)
 - ▣ En agrandissant un lun (on parle d' « expand »)

VMFS

33



VMFS

34

TP

Configuration d'un datastore VMFS

Les disques virtuels

35

- Fichiers composants une VM :
 - ▣ .vmx : fichier de configuration de la VM
 - ▣ .vmx.lck : fichier caché de lock
 - ▣ .nvram : configuration BIOS de la vM
 - ▣ .vmdk : disque de la VM
 - ▣ -000#.vmdk : fichier de post-snapshot
 - ▣ .vmss : dictionnaire des snapshots
 - ▣ .vmem : mémoire la VM
 - ▣ .vmss : utilisé quand la machine est en pause
 - ▣ -Snapshot#.vmsn : snapshot de la mémoire
 - ▣ .vswp : swap virtuel de la VM

Les disques virtuels

36

- Format des disques :
 - ▣ Thin
 - Le disque virtuel augmente au fur et à mesure que la VM en a besoin
 - ▣ Tick (zeroedthick)
 - Le VMDK fait sa taille maximum au niveau du datastore mais pas sur le disque
 - ▣ EagerZeroedTick
 - Le VMDK fait sa taille maximum au niveau du datastore et sur le disque (il est rempli de 0 à sa création)

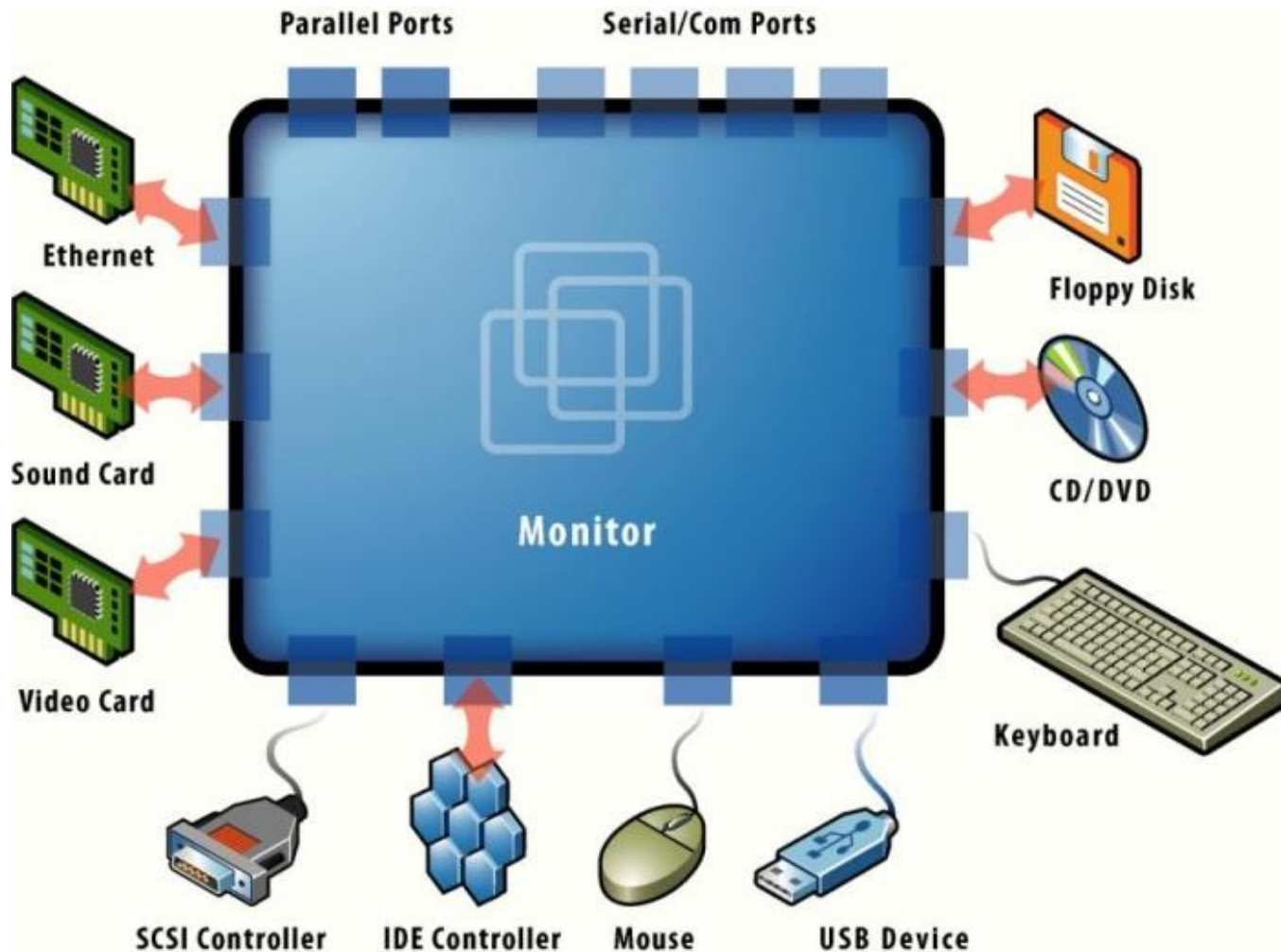
Création et gestion de VM

37

- Une VM utilise du matériel virtuel :
 - ▣ vSphere 6.7 = couche matérielle en version 14
 - ▣ Limites :
 - 128 vCPU
 - 6128Go de RAM
 - ▣ Limites en version 8 (vsphere 5.0) :
 - 8 vCPU
 - 256Go de RAM
- La version de matériel utilisé a un impact fort :
 - ▣ Sur les fonctionnalités disponibles (contrôleurs disques SAS, NVMe, ..)
 - ▣ Les instructions remontées dans le système d'exploitation invité : AVX, modes IBRS et STIBP pour les attaques spectre/meltdown

Création et gestion de VM

38



Création et gestion de VM

39

- Pour créer une nouvelle machine, il faut :
 - ▣ Un nom
 - ▣ Un type d'OS
 - ▣ Nombre de CPU
 - ▣ Taille de la RAM
 - ▣ Emplacement du disque virtuel et taille
- Le type d'OS permet à VMware de choisir automatiquement certains paramètres (ex : contrôleur SCSI)

Création et gestion de la VM

40

□ Le VMM et les overhead :

Memory (MB)	1 VCPU	2 VCPUs	3 VCPUs	4 VCPUs	5 VCPUs	6 VCPUs	7 VCPUs	8 VCPUs
256	113.17	159.43	200.53	241.62	293.15	334.27	375.38	416.50
512	116.68	164.96	206.07	247.17	302.75	343.88	385.02	426.15
1024	123.73	176.05	217.18	258.30	322.00	363.17	404.34	445.52
2048	137.81	198.20	239.37	280.53	360.46	401.70	442.94	484.18
4096	165.98	242.51	283.75	324.99	437.37	478.75	520.14	561.52
8192	222.30	331.12	372.52	413.91	591.20	632.86	674.53	716.19
16384	334.96	508.34	550.05	591.76	900.44	942.98	985.52	1028.07
32768	560.27	863.41	906.06	948.71	1515.75	1559.42	1603.09	1646.76
65536	1011.21	1572.29	1616.19	1660.09	2746.38	2792.30	2838.22	2884.14
131072	1912.48	2990.05	3036.46	3082.88	5220.24	5273.18	5326.11	5379.05
262144	3714.99	5830.60	5884.53	5938.46	10142.83	10204.79	10266.74	10328.69

Création et gestion de VM

41

- Installation de la VM :
 - ▣ Utilisation d'une image iso visible par le vCenter
 - ▣ Utilisation du lecteur de CD de l'ESXi
 - ▣ Utilisation du lecteur de CD de la machine qui a lancée le vSphere Client
 - ▣ Utilisation du boot PXE dans la VM

Création et gestion de VM

42

- Les VMware Tools:
 - ▣ Pilotes graphique + souris
 - ▣ Drivers réseaux et disque
 - ▣ Driver pour le ballooning mémoire
 - ▣ VM heart beat
 - ▣ Synchronisation du temps avec le serveur ESX (déprécié)
 - ▣ Arrêt/Démarrage/Reboot « propres »
 - ▣ Flush écritures disques lors des opérations de snapshot

Création et gestion de VM

43

TP

Installation d'une machine virtuelle

Les snapshots

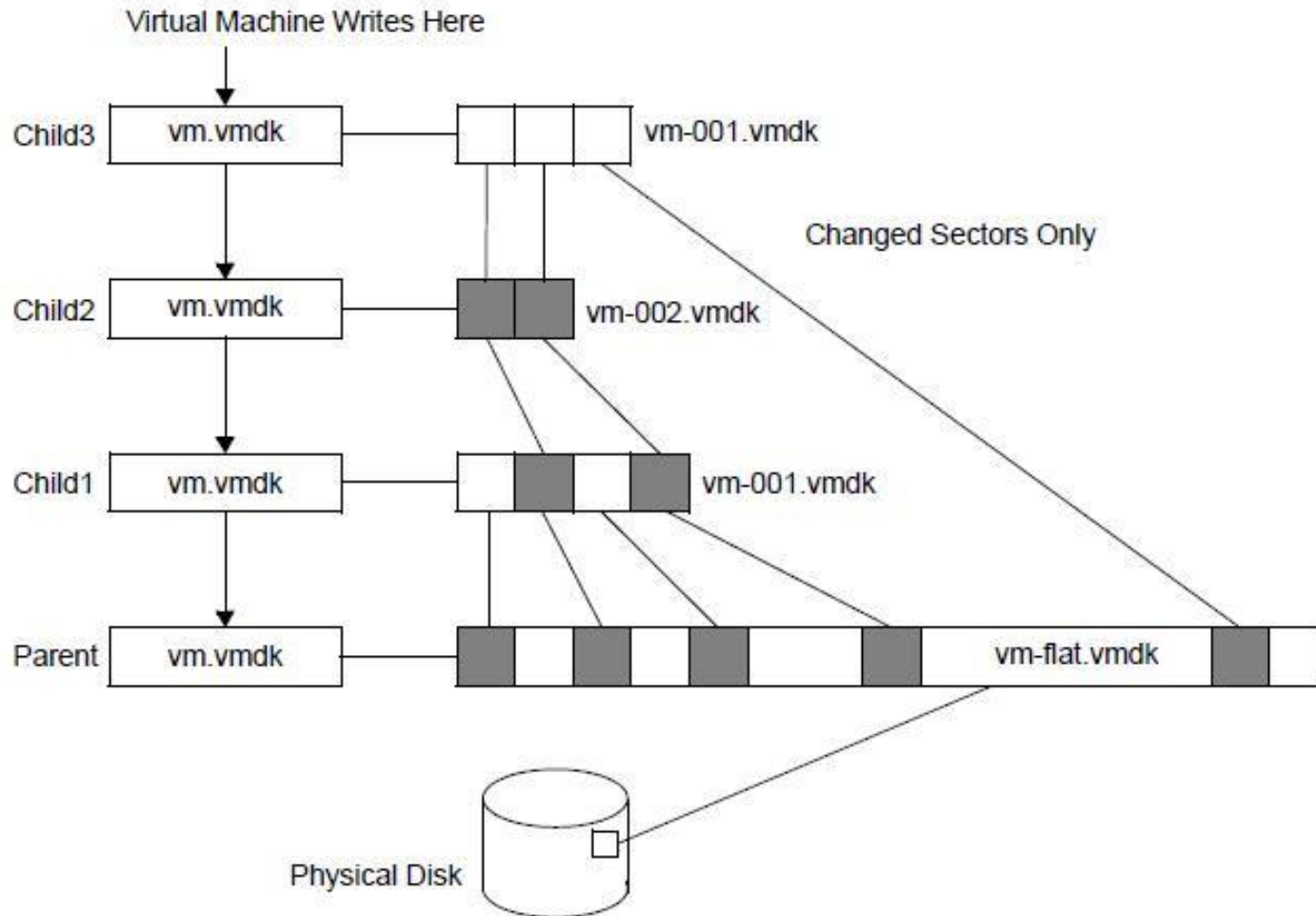
44

- Permettent de capturer à un instant T l'état de la machine :
 - ▣ La RAM
 - ▣ Le disque

- Les fichiers de snapshot -0000X.vmdk contiennent le delta entre des blocs du disque à l'instant T et les blocs du disque à l'instant T2

Les snapshots

45



Snapshots

46

TP

Création et gestion de snapshots

La gestion des CPU

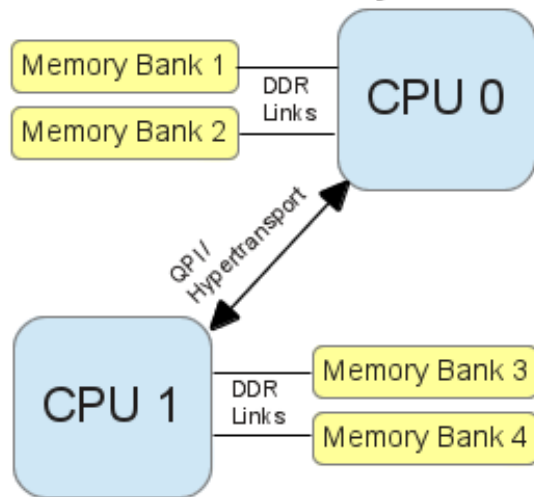
- Les impacts des architectures NUMA
- Le dimensionnement
- Diagnostiquer les problèmes de performances

Les architectures NUMA

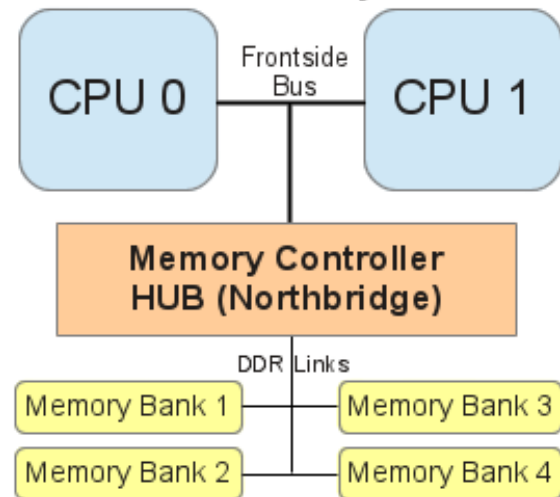
- **Non-Uniform Memory Access**
- Chaque CPU a une partie de RAM considérée comme « locale »
- Les CPU ont un accès privilégié à la RAM locale
- CPU récents (à partir de Nehalem, Opteron)
- Visible par ESXtop (mode mémoire)

NUMA vs UMA

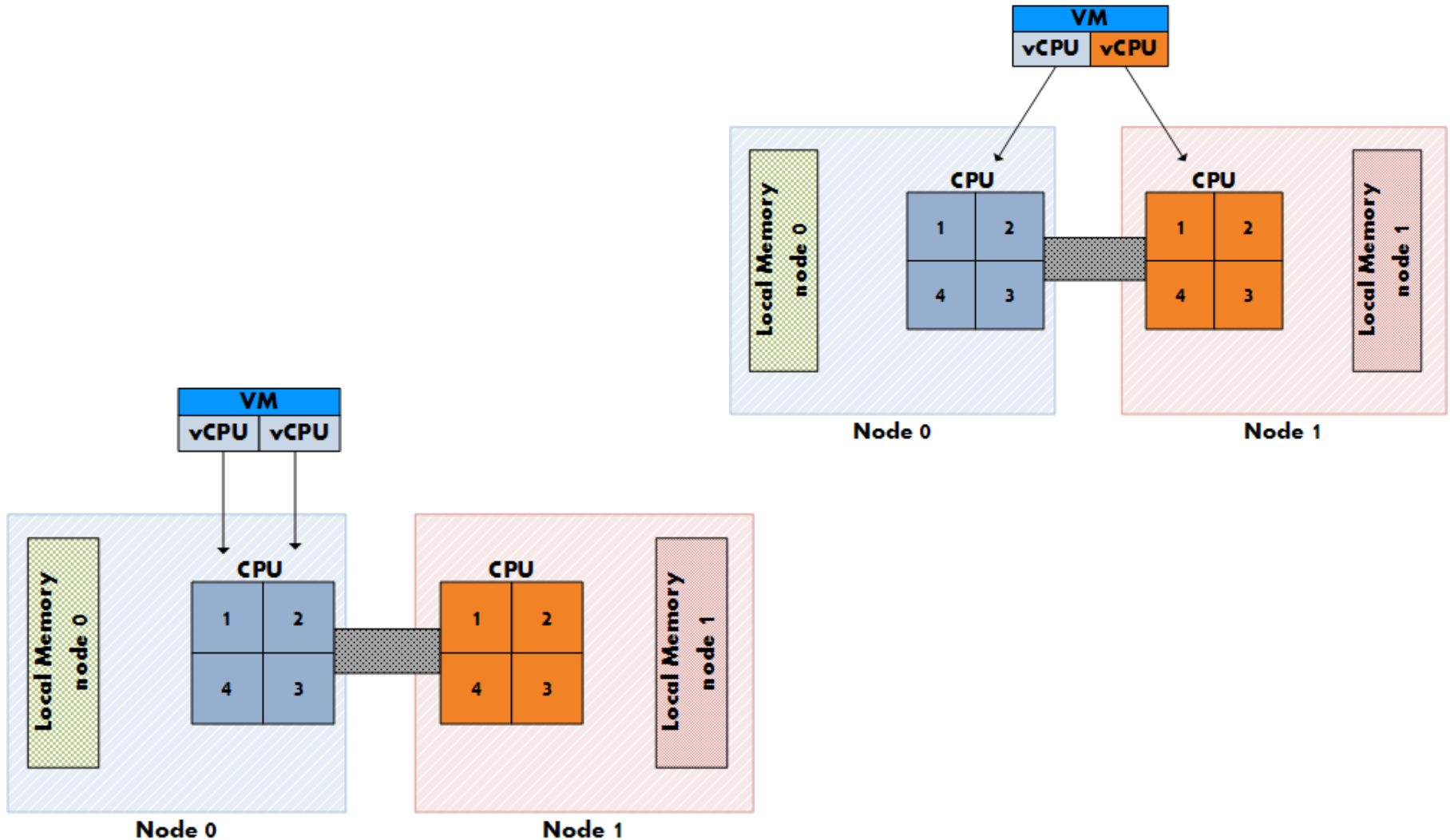
Non-Uniform Memory Access



Uniform Memory Access



NUMA - localité



Hardware-assisted CPU virtualization

- Le Binary translation (BT)
 - ▣ Permet de capturer les instructions privilégiées normalement gérées par l'OS dans le ring 0
 - ▣ On parle de « trap and emulate »

- Intel VT-x et AMD AMD-v (2006)
 - ▣ Hardware assisted virtualization (HV), on ajoute un ring (-1)

Les VM et la mémoire

- Deux niveaux de mémoire dans la VM :
 - ▣ Mémoire virtuelle (utilisé pour la première fois en 1959)
 - ▣ Mémoire physique
- La correspondance virtuelle <> physique est stockée dans la « page table » qui est stockée en mémoire

Les VM et la mémoire

- Si application a besoin de données, on fait un « page table walk » pour connaître la correspondance virtuelle <> physique
- Si la donnée n'est pas dans la mémoire physique (exemple : swap), on la récupère et on la met en mémoire physique

Les VM et la mémoire

- Le « page table walk » est assez lent alors pour résoudre le problème, on a inventé les **Memory Management Unit** et les **Translation Look-aside Buffer** (cache pour la MMU)

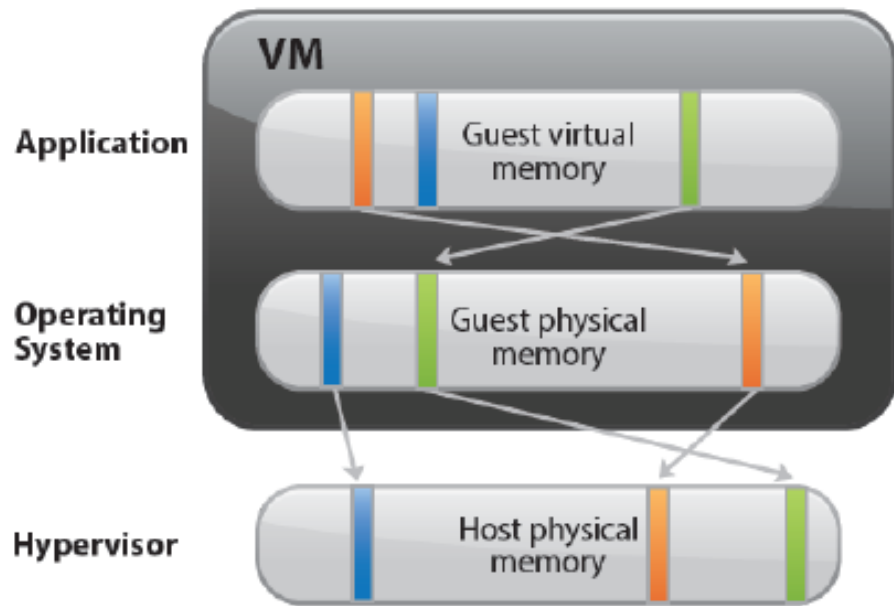
Les VM et la mémoire

- Problème : dans le cas d'un hyperviseur, nous avons un niveau de correspondance supplémentaire :
 - ▣ Mémoire physique de l'hyperviseur <> mémoire « physique » de la VM
- La VM ne peut pas vraiment accéder à un MMU physique, il est émulé par le VMM

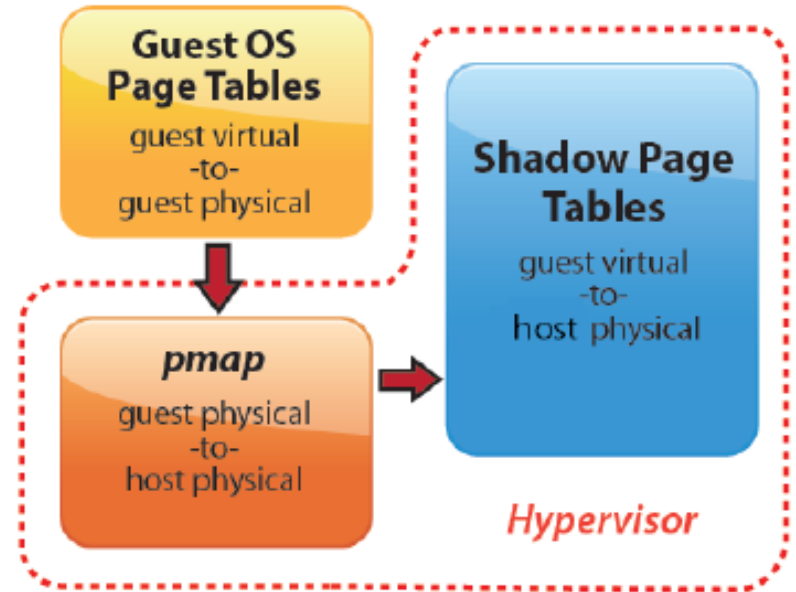
Les VM et la mémoire

- Le VMM est alors responsable du maintien de la correspondance :
 - ▣ Mémoire physique hyperviseur <> mémoire « physique VM »

Les VM et la mémoire



(a)



(b)

Créant la : Hardware-Assisted MMU virtualization .

Virtualisation du MMU

RVI ou NPT chez AMD

EPT chez Intel

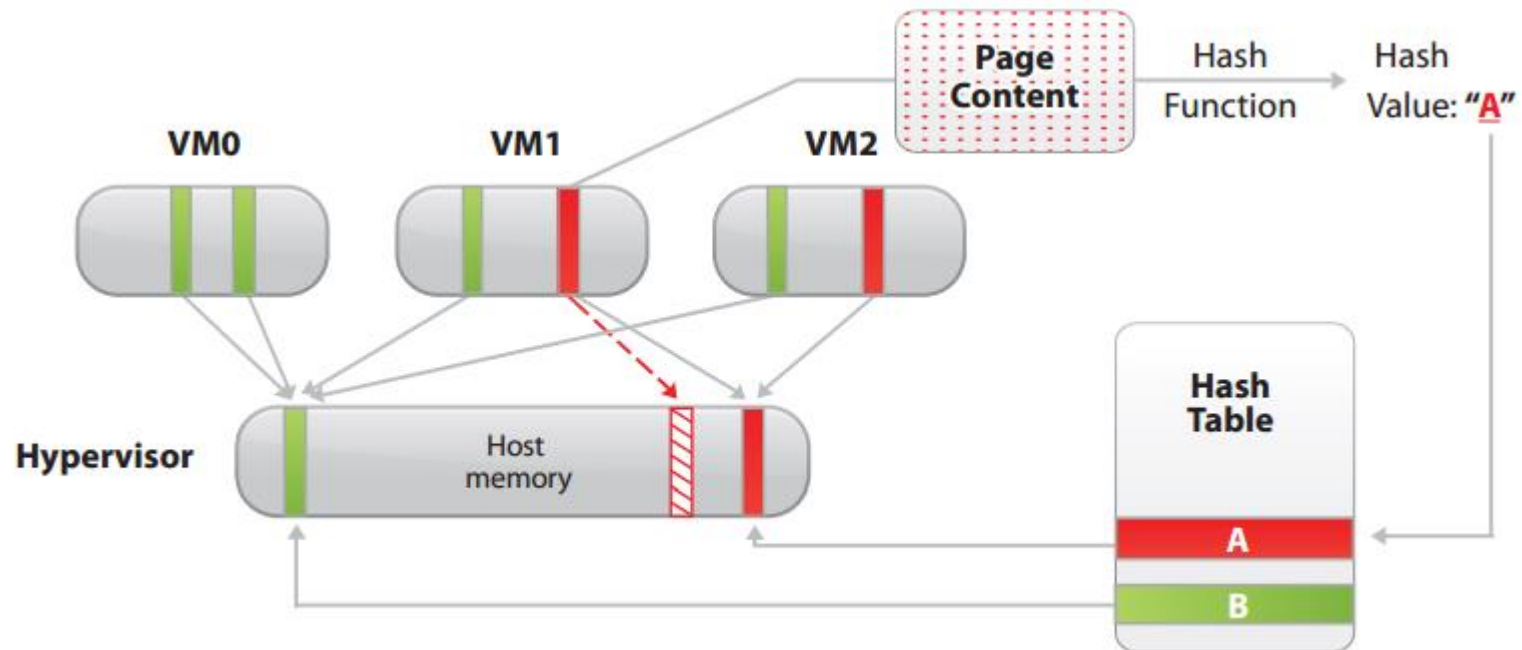
Hardware-Assisted MMU Virtualization



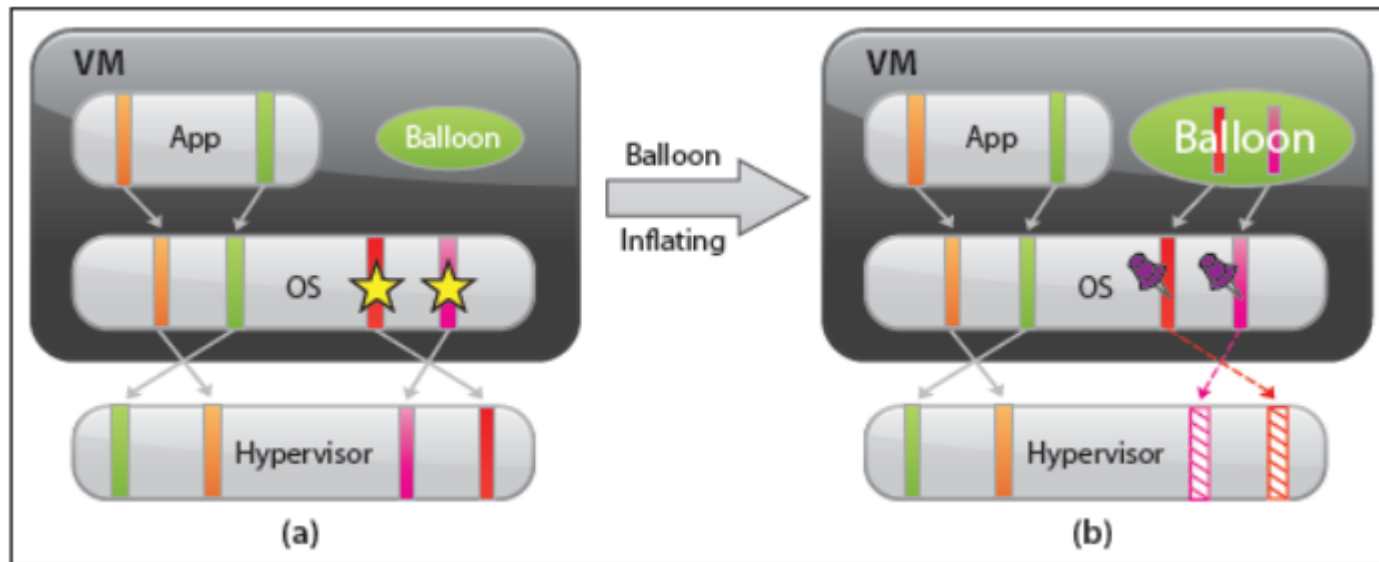
Transparent Page sharing

59

- Si on fait du HW assisted MMU :
 - ▣ Passage de 4KB à 2MB



Balloonning



Les templates

61

- Permet de créer des « masters »
 - ▣ On sauvegarde une configuration de VM ainsi qu'un ou plusieurs disques
 - ▣ Attention aux identifiants uniques générés pas certains OS (utilisez sysprep, ..)
- Un template ne peut pas être démarré
- On peut utiliser des scripts de personnalisation lors du déploiement d'un template

Les clones

62

- Permet de créer une copie identique d'une VM
- Peut être réalisé sur une VM en fonctionnement

Templates et clones

63

TP

Création et gestion de templates

Migration et import de VM

64

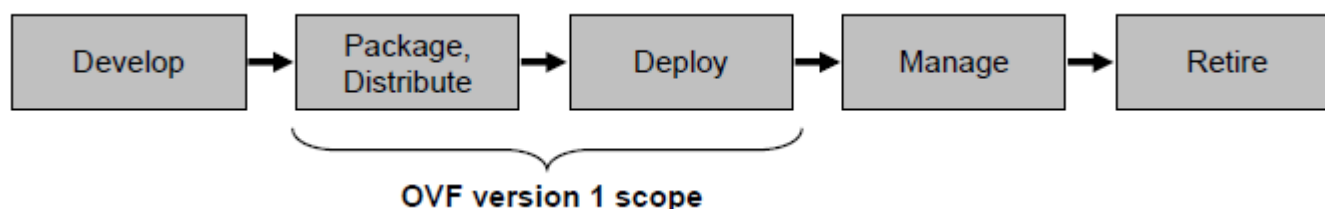
- Solution de P2V et V2V :
 - ▣ vCenter Converter :
 - Migration à chaud ou à froid
 - Pensez à faire le ménage après la migration
 - Adaptez la configuration matérielle de la VM
- Import d'appliances :
 - ▣ Open Virtual (Machine) Format
 - ▣ Exemples : www.vmware.com/appliances
 - ▣ F5, Cisco, Zimbra, ..

Les OVF

- Naissance en Septembre 2007 (Dell, IBM, Microsoft, VMware, XenSource) lors de la soumission à la DMTF
- Spec officielle depuis Janvier 2010
 - ▣ Supporté depuis ESX 3.5 (fin 2007)
- On parle de **package** OVF
 - ▣ Contient plusieurs fichiers dans un même répertoire (fichiers disques + xml)
 - ▣ OVA = OVF au format tar ou zip

Les OVF

- La place des OVF :



- Utilisation de disques partagés et de fichiers delta
- La personnalisation lors du déploiement :

Product	Property	Description
Linux	<i>hostname</i>	Network identity of the application, including IP address.
	<i>ip</i>	
	<i>subnet</i>	
	<i>gateway</i>	
	<i>dns</i>	
	<i>netCoreRmemMax</i>	Parameters to optimize the transfer rate of the IP stack
	<i>netCoreWmemMax</i>	

Sécurité d'accès au vCenter et aux VMs

67

- Les utilisateurs possèdent un rôle qui leur permet de réaliser des actions (Allumer une VM, Créer une VM, ..)
- Rôles par défaut pour un ESXi:
 - ▣ No Access
 - Permet d'exclure des utilisateurs
 - ▣ Read-Only
 - Permet de voir certaines configurations
 - ▣ Administrator
 - « Full power »

Sécurité d'accès au vCenter et aux VMs

68

- Rôles par défaut pour un vCenter:
 - ▣ Même que sur les ESX plus :
 - ▣ Virtual Machine Power user
 - Permet de faire toutes les opérations sur les VM
 - ▣ Virtual Machine User
 - Permet d'interagir avec la VM mais pas de la modifier
 - ▣ Resource Pool Administrator
 - Permet de gérer un Resource Pool et ses machines
 - ▣ VMware Consolidated Backup User
 - Permet d'utiliser des opérations de backup
 - ▣ Datastore Consumer
 - Permet d'utiliser de l'espace sur le(s) datastore(s)
 - ▣ Network Consumer
 - Permet de rattacher une VM a un réseau

TP

Gestion de la sécurité sous vSphere

Les alarmes

70

- Une alarme est caractérisée par :
 - ▣ Le ou les objet(s) sur lequel(s) elle s'applique
 - ▣ Un ou plusieurs « trigger »
 - ▣ L'action à réaliser

- 3 états :
 - ▣ Normal
 - ▣ Warning
 - ▣ Alert

- Réponses utilisateur :
 - ▣ Ignorer
 - ▣ Acknowledge (grisée)
 - ▣ Clear (disparait)

Les alarmes

71

- Les objets :
 - ▣ VM, Datastore, ...
 - ▣ Notion d'héritage

- Les triggers :
 - ▣ Condition
 - ▣ Événement

- Actions
 - ▣ Mail, trap, script, action sur la VM

TP

Gestion des alarmes

Gestion des logs

- Plusieurs types de logs :
 - ▣ vCenter
 - Différents services
 - ▣ ESXi
 - Stockés localement
 - Ephémères quand on utilise autodeploy

Les logs du vCenter

- Fichiers principaux de log du vCenter :
 - ▣ Vpxd
 - fichier de log principal
 - ▣ Vpx-profiler
 - Fichier de log des performances du vCenter
- Les fichiers sont visibles via le vSphere client

Les logs des ESXi

- Fichiers de log principaux :
 - ▣ /var/log/messages
 - Log de l'OS
 - ▣ /var/log/vmware/hostd.log
 - Log du Host Agent
 - ▣ /var/log/vmware/vpx/vpxa.log
 - Log de l'agent vCenter
- Rotation des fichiers de log

Les logs des ESXi

- Les logs sont accessibles :
 - ▣ Via la console du serveur
 - ▣ Via le vSphere client en cas de connexion directe
 - ▣ Via SSH (tail, ..)
 - ▣ Via Syslog (si activé)

Collecte des logs

- vCenter log bundle
 - ▣ Start -> Programs -> VMware
- ESXi log bundle
 - ▣ vSphere Client -> Administration -> Export system log
 - ▣ vm-support

TP

Gestion des logs

Outils d'administration

- Accès direct à l'ESX
 - ▣ vSphere Client
 - ▣ SSH
 - ▣ API

- Accès indirect
 - ▣ vCenter

SSH

- ESXi en mode console
- Accès aux commandes :
 - ▣ Esxcli
 - ▣ Esxcfg
 - ▣ Net-dvs
 - ▣ ..

TP

Utilisation SSH

Gestion des hôtes ESXi

- VMware Update Manager
- Les VIB
- Les Host profile
- Image builder
- VMware AutoDeploy

VUM

- VMware Update Manager
 - ▣ Application de patchs
 - ▣ Déploiement de mises à jour majeures d'ESXi
 - ▣ Mise à jour de Virtual Appliance
- Nécessite une installation du service et le déploiement du plugin

VUM

- Une baseline regroupe un ou plusieurs patches
- Les baselines groups regroupent des baselines
- 4 status pour les patches :
 - ▣ Unknow
 - ▣ Non-compliant
 - ▣ Compliant
 - ▣ Incompatible

VUM

- Les patches sont stockés dans un dépôt
- Les patches VMware sont téléchargés automatiquement à intervalle régulier
- On peut déposer des patches dans le dépôt ou des images d'ESXi

Les VIB

- **vSphere Installation Bundle**
- Packages logiciels pour les ESXi
 - ▣ Une archive
 - ▣ Un fichier XML de description
 - ▣ Un fichier de signature
- Peuvent être intégrés aux images via l'image builder

Les VIB

- 2 méthodes de déploiement
 - ▣ VUM
 - ▣ Esxcli (esxcli software vib install)

- Plusieurs niveaux d' 'acceptance'
 - ▣ Vmware certified
 - ▣ Vmware Accepted
 - ▣ Partner Supported
 - ▣ Community supported

TP

Déploiement d'un vib